

Tame Decompositions and Collisions

Konstantin Ziegler
 B-IT, Universität Bonn
 D-53113 Bonn, Germany
zieglerk@bit.uni-bonn.de
<http://cosec.bit.uni-bonn.de/>

February 25, 2014

Abstract

A univariate polynomial f over a field is decomposable if $f = g \circ h = g(h)$ for nonlinear polynomials g and h . It is intuitively clear that the decomposable polynomials form a small minority among all polynomials over a finite field. The tame case, where the characteristic p of \mathbb{F}_q does not divide $n = \deg f$, is fairly well-understood, and we have reasonable bounds on the number of decomposables of degree n . Nevertheless, no exact formula is known if n has more than two prime factors. In order to count the decomposables, one wants to know, under a suitable normalization, the number of collisions, where essentially different (g, h) yield the same f . In the tame case, Ritt's Second Theorem classifies all 2-collisions.

We introduce a normal form for multi-collisions of decompositions of arbitrary length with exact description of the (non)uniqueness of the parameters. We obtain an efficiently computable formula for the exact number of such collisions at degree n over a finite field of characteristic coprime to p . This leads to an algorithm for the exact number of decomposable polynomials at degree n over a finite field \mathbb{F}_q in the tame case.

1 Introduction

The *composition* of two univariate polynomials $g, h \in F[x]$ over a field F is denoted as $f = g \circ h = g(h)$, and then (g, h) is a *decomposition* of f , and f is *decomposable* if g and h have degree at least 2. In the 1920s, Ritt,

Fatou, and Julia studied structural properties of these decompositions over \mathbb{C} , using analytic methods. Particularly important are two theorems by Ritt on the uniqueness, in a suitable sense, of decompositions, the first one for (many) indecomposable components and the second one for two components, as above. Engstrom (1941) and Levi (1942) proved them over arbitrary fields of characteristic zero using algebraic methods.

The theory was extended to arbitrary characteristic by Fried & MacRae (1969), Dorey & Whaples (1974), Schinzel (1982, 2000), Zannier (1993), and others. Its use in a cryptographic context was suggested by Cade (1985). In computer algebra, the decomposition method of Barton & Zippel (1985) requires exponential time. A fundamental dichotomy is between the *tame case*, where the characteristic p does not divide $\deg g$, and the *wild case*, where p divides $\deg g$, see von zur Gathen (1990a,b). A breakthrough result of Kozen & Landau (1989) was their polynomial-time algorithm to compute tame decompositions; see also von zur Gathen, Kozen & Landau (1987); Kozen, Landau & Zippel (1996); Gutierrez & Sevilla (2006), and the survey articles of von zur Gathen (2002) and Gutierrez & Kozen (2003) with further references.

Schur's conjecture, as proven by Turnwald (1995), offers a natural connection between indecomposable polynomials with degree coprime to p and certain absolutely irreducible bivariate polynomials. On a different, but related topic, Avanzi & Zannier (2003) study ambiguities in the decomposition of rational functions over \mathbb{C} .

It is intuitively clear that the univariate decomposable polynomials form only a small minority among all univariate polynomials over a field. A set of distinct decompositions of f is called a *collision*. The number of decomposable polynomials of degree n is thus the number of all pairs (g, h) with $\deg g \cdot \deg h = n$ reduced by the ambiguities introduced by collisions. An important tool for estimating the number of collisions is Ritt's Second Theorem. Ritt worked with $F = \mathbb{C}$ and used analytic methods. Subsequently, his approach was replaced by algebraic methods and Ritt's Second Theorem was also shown to hold in positive characteristic p . The original versions of this required $p > \deg(g \circ h)$. Zannier (1993) reduced this to the milder and more natural requirement $g' \neq 0$ for all g in the collision. His proof works over an algebraic closed field, and Schinzel's (2000) monograph adapts it to finite fields.

The task of counting compositions over a finite field of characteristic p was first considered in Giesbrecht (1988). Von zur Gathen (2014a) presents general approximations to the number of decomposable polynomials. These come with satisfactory (rapidly decreasing) relative error bounds except when p divides $n = \deg f$ exactly twice. Blankertz, von zur Gathen & Ziegler (2013)

determine exactly the number of decomposable polynomials in one of these difficult cases, namely when $n = p^2$.

Zannier (2008) studies a different but related question, namely compositions $f = g \circ h$ in $\mathbb{C}[x]$ with a *sparse* polynomial f , having t terms. The degree is not bounded. He gives bounds, depending only on t , on the degree of g and the number of terms in h . Furthermore, he gives a parametrization of all such f, g, h in terms of varieties (for the coefficients) and lattices (for the exponents). Bodin, Dèbes & Najib (2009) also deal with counting.

Zieve & Müller (2008) derive an efficient method for describing all complete decompositions of a polynomial, where all components are indecomposable. This turns Ritt’s First Theorem into an applicable form and Medvedev & Scanlon (2014) combine this approach with results from model theory to describe the subvarieties of the k -dimensional affine space that are preserved by a coordinatewise polynomial map. Both works lead to slightly different canonical forms for the complete decomposition of a given polynomial. Zieve & Müller (2008) employ *Ritt moves*, where adjacent indecomposable g, h in a complete decomposition are replaced by g^*, h^* with the same composition, but $\deg g = \deg h^* \neq \deg h = \deg g^*$. Such collisions are the theme of Ritt’s Second Theorem and von zur Gathen (2014b) presents a normal form with an exact description of the (non)uniqueness of the parameters.

Our work combines the “normalizations” of Ritt’s theorems by Zieve & Müller (2008) and von zur Gathen (2014b) to classify collisions of two or more decompositions, not necessarily complete and of arbitrary length. We make the following contributions.

- We obtain a normal form for collisions described by a set of degree sequences for (possibly incomplete) decompositions. (Theorem 3.14 and Theorem 3.15)
- The (non)uniqueness of the parameters leads to an exact formula for the number of such collisions over a finite field with characteristic coprime their degree. (Theorem 4.1)
- We conclude with an efficient algorithm for the number of decomposable polynomials at degree n over a finite field of characteristic coprime n . (Algorithm 4.2)

The latter extends the explicit formulae of von zur Gathen (2014a) for n a semiprime or the cube of a prime.

We proceed in three steps. In Section 2, we introduce notation and establish basic relations. In Section 3, we introduce the *relation graph* of a set of collisions which captures the necessary order and possible Ritt moves for

any in decomposition. This leads to a complete classification of collisions by Theorem 3.14 and Theorem 3.15. We conclude with the corresponding formula for the number of such collisions over a finite field and the corresponding procedure in Section 4.

2 Notation and Preliminaries

A nonzero polynomial $f \in F[x]$ over a field F of characteristic $p \geq 0$ is *monic* if its leading coefficient $\text{lc}(f)$ equals 1. We call f *original* if its graph contains the origin, that is, $f(0) = 0$. For $g, h \in F[x]$,

$$f = g \circ h = g(h) \in F[x] \quad (2.1)$$

is their *composition*. If $\deg g, \deg h \geq 2$, then (g, h) is a *decomposition* of f . A polynomial $f \in F[x]$ is *decomposable* if there exist such g and h , otherwise f is *indecomposable*. A decomposition (2.1) is *tame* if $p \nmid \deg g$, and f is *tame* if $p \nmid \deg f$.

Multiplication by a unit or addition of a constant does not change decomposability, since

$$f = g \circ h \iff af + b = (ag + b) \circ h$$

for all f, g, h as above and $a, b \in F$ with $a \neq 0$. In other words, the set of decomposable polynomials is invariant under this action of $F^\times \times F$ on $F[x]$. Furthermore, any decomposition (g, h) can be normalized by this action, by taking $a = \text{lc}(h)^{-1} \in F^\times$, $b = -a \cdot h(0) \in F$, $g^* = g((x - b)a^{-1}) \in F[x]$, and $h^* = ah + b$. Then $g \circ h = g^* \circ h^*$ and g^* and h^* are monic original.

It is therefore sufficient to consider compositions $f = g \circ h$ where all three polynomials are monic original. For $n \geq 1$ and any positive divisor d of n , we write

$$\begin{aligned} \mathcal{P}_n(F) &= \{f \in F[x] : f \text{ is monic original of degree } n\}, \\ \mathcal{D}_n(F) &= \{f \in \mathcal{P}_n : f \text{ is decomposable}\}, \\ \mathcal{D}_{n,d}(F) &= \{f \in \mathcal{P}_n : f = g \circ h \text{ for some } (g, h) \in \mathcal{P}_d \times \mathcal{P}_{n/d}\}. \end{aligned}$$

We sometimes leave out F from the notation when it is clear from the context and have over a finite field \mathbb{F}_q with q elements,

$$\#\mathcal{P}_n = q^{n-1}. \quad (2.1a)$$

It is well known that in a tame decomposition, g and h are uniquely determined and we have over \mathbb{F}_q

$$\#\mathcal{D}_{n,d} = q^{n+n/d-2} \quad (2.2)$$

if n is coprime to p .

The set \mathcal{D}_n of all decomposable polynomials in \mathcal{P}_n satisfies

$$\mathcal{D}_n = \bigcup_{\substack{d|n \\ 1 < d < n}} \mathcal{D}_{n,d}. \quad (2.3)$$

In particular, $\mathcal{D}_n = \emptyset$ if n is prime. Our collisions turn up in the resulting inclusion-exclusion formula for $\#\mathcal{D}_n$ if n is composite.

Let $N = \{1 < d < n : d \mid n\}$ be the set of nontrivial divisors of n and $D \subseteq N$ a nonempty subset of size k . This defines a set

$$\mathcal{D}_{n,D} = \bigcap_{d \in D} \mathcal{D}_{n,d}$$

of k -collisions. We obtain from (2.3) the inclusion-exclusion formula

$$\#\mathcal{D}_n = \sum_{k \geq 1} (-1)^{k+1} \sum_{\substack{D \subseteq N \\ \#D=k}} \#\mathcal{D}_{n,D}. \quad (2.4)$$

For $\#D = 1$, the size of $\mathcal{D}_{n,D}$ is given in (2.2). For $\#D = 2$, the central tool for understanding is Ritt's Second Theorem as presented in the next subsection.

For $f \in P_n(F)$ and $a \in F$, the *original shift* of f by a is

$$f^{[a]} = (x - f(a)) \circ f \circ (x + a) \in \mathcal{P}_n(F). \quad (2.5)$$

Original shifting defines a group action of the additive group of F on $\mathcal{P}_n(F)$. Shifting respects decompositions in the sense that for each decomposition (g, h) of f we have a decomposition $(g^{[h(a)]}, h^{[a]})$ of $f^{[a]}$, and vice versa. We denote $(g^{[h(a)]}, h^{[a]})$ as $(g, h)^{[a]}$. The stabilizer of a monic original polynomial f under original shifting is F if f is linear and $\{0\}$ otherwise.

2.1 Normal Form for Ritt's Second Theorem

In the 1920s, Ritt, Fatou, and Julia investigated the composition $f = g \circ h = g(h)$ of univariate polynomials over a field F for $F = \mathbb{C}$. It emerged as an important question to determine the collisions (or nonuniqueness) of such decompositions, that is, different components $(g, h) \neq (g^*, h^*)$ with equal composition $g \circ h = g^* \circ h^*$ and equal sets of degrees: $\deg g = \deg h^* \neq \deg h = \deg g^*$.

Ritt (1922) presented two types of essential collisions:

$$x^e \circ x^k w(x^e) = x^{ke} w^e(x^e) = x^k w^e \circ x^e, \quad (2.6)$$

$$T_d^*(x, z^e) \circ T_e^*(x, z) = T_{ed}^*(x, z) = T_e^*(x, z^d) \circ T_d^*(x, z), \quad (2.7)$$

where $w \in F[x]$, $z \in F^\times = F \setminus \{0\}$, and T_d^* is the d th *Dickson polynomial of the first kind*. And then he proved that these are all possibilities up to composition with linear polynomials. This involved four unspecified linear functions, and it is not clear whether there is a relation between the first and the second type of example. Without loss of generality, we use the *originalized* d th *Dickson polynomial* $T_d(x, z) = T_d^*(x, z) - T_d^*(0, z)$ which also satisfy (2.7).

Von zur Gathen (2014b) presents a normal form for the decompositions in Ritt's Theorem under Zannier's assumption $g'(g^*)' \neq 0$ and the standard assumption $\gcd(e, d) = 1$, where $d = k + e \deg w$ in (2.6). This normal form is unique unless $p \mid m$.

Theorem 2.8. (*Ritt's Second Theorem, Normal Form, tame case*) *Let $d > e \geq 2$ be coprime integers, and $n = de$ coprime to the characteristic of F . Furthermore, let $f = g \circ h = g^* \circ h^*$ be monic original polynomials with $\deg g = \deg h^* = d$, $\deg h = \deg g^* = e$.*

Then either (i) or (ii) holds, and (iii) is also valid.

- (i) (*Exponential Case*) *There exists a monic polynomial $w \in F[x]$ of degree s and $a \in F$ so that*

$$f = (x^{ke} w^e(x^e))^{[a]}$$

where $d = se + k$ is the division with remainder of d by e , with $1 \leq k < e$. Furthermore

$$(g, h) = (x^k w^e, x^e)^{[a]}, \quad (g^*, h^*) = (x^e, x^k w(x^e))^{[a]},$$

and (w, a) is uniquely determined by f and d . Conversely, any (w, a) as above yields a 2-collision via the above formulas.

- (ii) (*Trigonometric Case*) *There exist $z, a \in F$ with $z \neq 0$ so that*

$$f = T_n(x, z)^{[a]}.$$

Furthermore we have

$$(g, h) = (T_d(x, z^e), T_e(x, z))^{[a]}, \quad (g^*, h^*) = (T_e(x, z^d), T_d(x, z))^{[a]},$$

and (z, a) is uniquely determined by f . Conversely, any (z, a) as above yields a 2-collision via the above formulas.

- (iii) *For $e = 2$, the Trigonometric Case is included in the Exponential Case. For $e \geq 3$, the Exponential and Trigonometric Cases are mutually exclusive.*

If $p \nmid n$, then the case where $\gcd(d, e) \neq 1$ is reduced to the previous one by the following result about the left and right greatest common divisors of decompositions. It was shown over algebraically closed fields by Tortrat (1988, Proposition 1); a more concise proof using Galois theory is due to Zieve & Müller (2008, Lemma 2.8). We use the version of von zur Gathen (2014b, Fact 6.1(i)), adapted to monic original polynomials.

Proposition 2.9. *Let $d, e, d^*, e^* \geq 2$ be integers and $de = d^*e^*$ coprime to p . Furthermore, let $g \circ h = g^* \circ h^*$ be monic original polynomials with $\deg g = d$, $\deg h = e$, $\deg g^* = d^*$, $\deg h^* = e^*$, and $\ell = \gcd(d, d^*)$, $r = \gcd(e, e^*)$. Then there are unique monic original polynomials a and b of degree ℓ and r , respectively, such that*

$$\begin{aligned} g &= a \circ u, & h &= v \circ b, \\ g^* &= a \circ u^*, & h^* &= v^* \circ b, \end{aligned}$$

for unique monic original polynomials u, u^*, v, v^* of degree d/ℓ , d^*/ℓ , e/r , and e^*/r , respectively.

This determines $\mathcal{D}_{n, \{d, e\}}$ exactly if $p \nmid n = de$.

For coprime integers $d \geq 2$ and $e \geq 1$, we define the sets

$$\begin{aligned} \mathcal{E}_{d, e} &= \begin{cases} \mathcal{P}_d & \text{for } e = 1, \\ \{x^k w^e \in \mathcal{P}_d : d = s \cdot e + k \text{ with } 1 \leq k < e \\ \text{and } w \in \mathbb{F}_q[x] \text{ monic of degree } s\}, & \text{otherwise,} \end{cases} \\ \mathcal{T}_{d, e} &= \{T_d(x, z^e) \in \mathcal{P}_d : z \in \mathbb{F}_q^\times\} \end{aligned} \quad (2.10)$$

of *exponential* and *trigonometric components*, respectively. For $d < e$, we have $s = 0$, $k = d$ in (2.10), and therefore

$$\mathcal{E}_{d, e} = \{x^d\}. \quad (2.10a)$$

This allows the following reformulation of Theorem 2.8.

Corollary 2.11. *Let $f \in \mathcal{D}_{n, \{d, e\}}$. Then either (i) or (ii) holds and (iii) is also valid.*

(i) *There is a unique monic original $g \in \mathcal{E}_{d, e}$ and a unique $a \in F$ such that*

$$f = (g \circ x^e)^{[a]}.$$

(ii) There is a unique monic original $g \in \mathcal{T}_{de,1}$ and a unique $a \in F$ such that

$$f = g^{[a]}.$$

(iii) If $e = 2$, then case (ii) is included in case (i). If $e \geq 3$, they are mutually exclusive.

Conversely, we have

$$\mathcal{D}_{n,\{d,e\}} = (\mathcal{E}_{d,e} \circ \mathcal{E}_{e,d})^{[F]} \cup \mathcal{T}_{de,1}^{[F]},$$

where the union is disjoint if and only if $e \geq 3$, and

$$\#\mathcal{D}_{n,\{d,e\}} = q \cdot (q^{\lfloor d/e \rfloor} + (1 - \delta_{e,2})(q - 1)).$$

With respect to the size under original shifting, we have the following consequences.

Proposition 2.14. For $F = \mathbb{F}_q$, coprime $d \geq 2$ and $e \geq 1$, both coprime to p , we have

$$\begin{aligned} \#\mathcal{T}_{d,e}^{[\mathbb{F}_q]} &= \begin{cases} q & \text{for } d = 2, \\ q(q-1)/\gcd(q-1, e) & \text{otherwise,} \end{cases} \\ \#\mathcal{E}_{d,e}^{[\mathbb{F}_q]} &= \begin{cases} q^{d-1} & \text{for } e = 1, \\ q^{\lfloor d/2 \rfloor + 1} - q(q-1)/2 & \text{for } e = 2, \\ q^{\lfloor d/e \rfloor + 1} & \text{otherwise.} \end{cases} \end{aligned}$$

Proof. (i) For $d = 2$, we have $\mathcal{T}_{2,e} = \{x^2\}$ independent from e . Since $p \neq 2$, the original shifts $(x^2)^{[a]} = x^2 + 2ax$ range over all monic original polynomials of degree 2 as a runs over all field elements. Thus $\mathcal{T}_{2,e}^{[F]} = \mathcal{P}_2$ and the size follows from (2.1a).

For $d > 2$, the coefficient of x^{d-2} in $T_d(x, z^e) \in \mathcal{T}_{d,e}$ is $-dz^e$. Since there are exactly $(q-1)/\gcd(q-1, e)$ distinct e th powers z^e for nonzero elements $z \in \mathbb{F}_q$, this shows

$$\#\mathcal{T}_{d,e} = (q-1)/\gcd(q-1, e).$$

For the claimed formula it is sufficient to show that for $T \in \mathcal{T}_{d,e}$ and $a \in F$, we have

$$T^{[a]} \in \mathcal{T}_{d,e} \text{ if and only if } a = 0.$$

For d odd, we also have T an odd polynomial. Hence the coefficient of x^{d-1} in T is 0 and the coefficient of x^{d-1} in $T^{[a]}$ is ad . This proves the claim. For d even, the same argument applies with “odd” replaced by “even”.

For a nonzero polynomial $f \in F[x]$ and b in some algebraic closure K of F , let $\text{mult}_b(f)$ denote the *root multiplicity* of b in f , so that $f = (x - b)^{\text{mult}_b(f)}u$ with $u \in K[x]$ and $u(b) \neq 0$.

(ii) For $e = 1$, we have $\mathcal{E}_{d,e} = \mathcal{P}_d = \mathcal{P}_d^{[F]}$ of size q^{d-1} by (2.1a).

For $e > 1$, we have $\#\mathcal{E}_{d,e} = q^{\lfloor d/e \rfloor}$. It is sufficient to show that for $f \in \mathcal{E}_{d,e}$ and $a \in F$, we have

$$f^{[a]} \in \mathcal{E}_{d,e} \text{ if and only if } a = 0.$$

We have directly $f^{[0]} = f \in \mathcal{E}_{d,e}$. Conversely, let $f^{[a]} = \bar{f} = x^k \bar{w}^e \in \mathcal{E}_{d,e}$, and compare the derivatives

$$\begin{aligned} f^{[a]'} &= (x+a)^{k-1} w(x+a)^{e-1} (kw(x+a) + e(x+a)w'(x+a)), \\ \bar{f}' &= x^{k-1} \bar{w}^{e-1} (k\bar{w} + ex\bar{w}'), \end{aligned}$$

respectively. These are nonzero, since $p \nmid d = \deg(\bar{f}) = \deg(f^{[a]})$, and we compute the root multiplicity of 0 as

$$\text{mult}_0(f^{[a]'}) = [a=0] \cdot (k-1) + \text{mult}_a(w) \cdot (e-1) + \begin{cases} \text{mult}_a(w) & \text{if } p \mid \text{mult}_a(w), \\ \text{mult}_a(w) - [a \neq 0] & \text{otherwise.} \end{cases}$$

$$= e \text{mult}_a(w) + [a=0](k-1) - [p \nmid \text{mult}_a(w) \text{ and } a \neq 0],$$

$$\begin{aligned} \text{mult}_0(\bar{f}') &= k-1 + (e-1) \cdot \text{mult}_0(\bar{w}) + \text{mult}_0(\bar{w}) \\ &= e \text{mult}_0(\bar{w}) + k-1. \end{aligned}$$

If $f^{[a]} = \bar{f}$, we find modulo e

$$k-1 = [a=0] \cdot (k-1) - [p \nmid \text{mult}_a(w) \text{ and } a \neq 0].$$

This holds if

- $a = 0$ or
- $p \mid \text{mult}_a(w)$ and $k = 1$.

It remains to show that the latter case is included in the former. In other words, that $p \mid \text{mult}_a(w)$ and $k = 1$ imply $a = 0$. Let $\Delta = w(x + a) - \bar{w}$ of degree less than s , since both are monic. Then

$$\begin{aligned} 0 = f^{[a]'} - \bar{f}' &= w(x + a)^e - \bar{w}^e + e((x + a)w'(x + a) - x\bar{w}') \\ &= e\Delta\bar{w}^{e-1} + \binom{e}{2}\Delta^2\bar{w}^{e-2} + \dots \\ &\quad + (e - 1)x\bar{w}' + ex\Delta' + ea\bar{w}' + ea\Delta' \end{aligned}$$

If $\Delta = 0$, we are done. Otherwise, $\deg \Delta \geq 0$ and the coefficient of $x^{\deg \Delta + s(e-1)}$ is

$$e \text{lc}(\Delta) + s(e - 1)[e = 2 \text{ and } \deg \Delta = 0].$$

If $e > 2$, this is nonzero, a contradiction.

We have $w(x + a) = \bar{w}$. Feeding this and $k = 1$ back into the definition of $f^{[a]}$ and \bar{f} , we obtain for their difference

$$f^{[a]} - \bar{f} = (x + a)\bar{w}^e - f(a) - x\bar{w}^e = a\bar{w}^e - f(a).$$

With $\deg(w) = s > 0$ this implies $a = 0$.

□

3 Normal Form for Collisions

The results of the previous section suffice to describe 2-collisions of decompositions $g \circ h = g^* \circ h^*$ with length 2 each. This section describes the structure of “many”-collisions of decompositions with arbitrary, possibly pairwise distinct, lengths. Let $\mathbf{d} = (d_1, d_2, \dots, d_\ell)$ be an ordered factorization of $n = d_1 \cdot d_2 \cdot \dots \cdot d_\ell$ with ℓ nontrivial divisors $d_i \in N$, $1 \leq i \leq \ell$, and define the set

$$\mathcal{D}_{n,\mathbf{d}} = \{f \in \mathcal{P}_n : f = g_1 \circ \dots \circ g_\ell \text{ with } \deg g_i = d_i \text{ for all } 1 \leq i \leq \ell\}$$

of decomposable polynomials with decompositions of *length* ℓ and *degree sequence* \mathbf{d} . For a set $\mathbf{D} = \{\mathbf{d}^{(1)}, \mathbf{d}^{(2)}, \dots, \mathbf{d}^{(c)}\}$ of c ordered factorizations of n , we define

$$\mathcal{D}_{n,\mathbf{D}} = \bigcap_{\mathbf{d} \in \mathbf{D}} \mathcal{D}_{n,\mathbf{d}}$$

$$= \{f \in \mathcal{P}_n : f = g_1^{(k)} \circ \cdots \circ g_{\ell_k}^{(k)} \text{ with } \deg g_i^{(k)} = d_i^{(k)} \\ \text{for all } 1 \leq k \leq c \text{ and } 1 \leq i \leq \ell_k\}.$$

For $\#D = 1$, we have

$$\mathcal{D}_{n,D} = \mathcal{D}_{n,d} = \mathcal{P}_{d_1} \circ \mathcal{P}_{d_2} \circ \cdots \circ \mathcal{P}_{d_\ell}, \\ \#\mathcal{D}_{n,D} = \#\mathcal{D}_{n,d} = q^{\sum_{1 \leq i \leq \ell} d_i - \ell},$$

where $D = \{d\}$ and $d = (d_1, d_2, \dots, d_\ell)$. The rest of this section deals with $\#D > 1$.

We determine the structure of $\mathcal{D}_{n,D}$. First, we replace D by a *refinement* D^* , where all elements are suitable permutations of the *same* ordered factorization of n . Second, we define the *relation graph* of D^* that captures the degree sequences for polynomials in $\mathcal{D}_{n,D}$. Finally, we classify the elements of $\mathcal{D}_{n,D}$ as a composition of unique trigonometric or unique exponential components as defined in (2.10).

3.1 A refinement of D

Let $d = (d_1, d_2)$ and $e = (e_1, e_2)$ be distinct ordered factorizations of n . Let $\ell = \gcd(d_1, e_1)$, $d_1^* = d_1/\ell$, $e_1^* = e_1/\ell$, $r = \gcd(d_2, e_2)$, $d_2^* = d_2/r$, and $e_2^* = e_2/r$. Then Proposition 2.9 shows

$$\mathcal{D}_{n,\{d,e\}} = \mathcal{D}_{n,\{d^*,e^*\}}$$

for $d^* = (\ell, d_1^*, d_2^*, r)$ and $e^* = (\ell, e_1^*, e_2^*, r)$ with $\gcd(d_1^*, e_1^*) = 1 = \gcd(d_2^*, e_2^*)$ and therefore $d_1^* = e_2^*$ and $d_2^* = e_1^*$. We generalize this procedure to two ordered factorizations of arbitrary length. For squarefree n this is similar to the computation of a coprime (also: gcd-free) basis for $\{d_1, d_2, e_1, e_2\}$, if we keep duplicates and the order of factors; see Bach & Shallit (1997, Section 4.8). For squareful n , the factors with $\gcd > 1$ require additional attention.

Let $d = (d_1, d_2, \dots, d_\ell)$ be an ordered factorization of n and call the underlying unordered multiset $\underline{d} = \{d_1, d_2, \dots, d_\ell\}$ of divisors its *basis*. A *refinement* of d is an ordered factorization $d^* = (d_{11}^*, \dots, d_{1m_1}^*, d_{21}^*, \dots, d_{2m_2}^*, \dots, d_{\ell 1}^*, \dots, d_{\ell m_\ell}^*)$, where $d_i = \prod_{1 \leq k \leq m_i} d_{ik}^*$ for all $1 \leq i \leq \ell$. We write $d^* \mid d$ and have directly

$$\mathcal{D}_{n,d^*} \subseteq \mathcal{D}_{n,d}. \quad (3.1)$$

Every ordered factorization is a refinement of (n) . A *complete* refinement of $d = (d_i)_{1 \leq i \leq \ell}$ is obtained by replacing every d_i by one of its ordered factorization into primes.

Two ordered factorizations $\mathbf{d} = (d_1, \dots, d_\ell)$ and $\mathbf{e} = (e_1, \dots, e_\ell)$ of n with the same basis, define a permutation $\sigma = \sigma(\mathbf{d}, \mathbf{e})$ on the indices $1, 2, \dots, \ell$ through

$$d_i = e_{\sigma(i)} \quad (3.2)$$

for $1 \leq i \leq \ell$. We require

$$\sigma(i) < \sigma(j) \text{ for all } i < j \text{ with } d_i = d_j \quad (3.3)$$

to make σ unique. In other words, σ has to preserve the order of repeated divisors. If even stronger,

$$\sigma(i) < \sigma(j) \text{ for all } i < j \text{ with } \gcd(d_i, d_j) > 1, \quad (3.4)$$

then we call \mathbf{d} and \mathbf{e} *associated*. Any two complete refinements \mathbf{d}^* of \mathbf{d} and \mathbf{e}^* of \mathbf{e} , respectively, are associated and we have from (3.1)

$$\mathcal{D}_{n, \{\mathbf{d}^*, \mathbf{e}^*\}} \subseteq \mathcal{D}_{n, \{\mathbf{d}, \mathbf{e}\}}. \quad (3.5)$$

We ask for associated refinements \mathbf{d}^* and \mathbf{e}^* , respectively, that describe the same set of collisions as \mathbf{d} and \mathbf{e} . Algorithm 3.6 solves this task and returns “coarsest” associated refinements \mathbf{d}^* and \mathbf{e}^* that yield equality in (3.5). We call the output \mathbf{d}^* of Algorithm 3.6 the *refinement of \mathbf{d} by \mathbf{e}* and denote it by $\mathbf{d}^* = \mathbf{d} \parallel \mathbf{e}$. Similarly, $\mathbf{e}^* = \mathbf{e} \parallel \mathbf{d}$ is the refinement of \mathbf{e} by \mathbf{d} and this is well-defined, since interchanging the order of the input merely interchanges the order of the output.

Lemma 3.7. *For two ordered factorizations \mathbf{d} and \mathbf{e} of n , the following are equivalent.*

- (i) $\text{len}(\mathbf{d} \parallel \mathbf{e}) = \text{len}(\mathbf{d})$ and $\text{len}(\mathbf{e} \parallel \mathbf{d}) = \text{len}(\mathbf{e})$.
- (ii) $\mathbf{d} \parallel \mathbf{e} = \mathbf{d}$ and $\mathbf{e} \parallel \mathbf{d} = \mathbf{e}$.
- (iii) \mathbf{d} and \mathbf{e} are associated.

Proof. Let $\mathbf{d} = (d_1, \dots, d_\ell)$ and $\mathbf{e} = (e_1, \dots, e_\ell)$ be associated and $\sigma = \sigma(\mathbf{d}, \mathbf{e})$ the unique permutation satisfying (3.2) and (3.4). Then we have in step 5 of Algorithm 3.6

$$\gcd(d_{i,m+1}^*, e_{j,\ell+1}^*) = \begin{cases} d_i = e_j & \text{if } j = \sigma(i), \\ 1 & \text{otherwise,} \end{cases}$$

for all $1 \leq i \leq \ell$ and $1 \leq j \leq m$. Thus Algorithm 3.6 returns \mathbf{d}, \mathbf{e} on input \mathbf{d}, \mathbf{e} and (ii) and (i) follow.

Algorithm 3.6: Refine \mathbf{d} and \mathbf{e}

Input: two ordered factorizations $\mathbf{d} = (d_1, \dots, d_\ell)$ and $\mathbf{e} = (e_1, \dots, e_m)$ of n

Output: two associated refinements $\mathbf{d}^* \mid \mathbf{d}$ and $\mathbf{e}^* \mid \mathbf{e}$

```

1  $\mathbf{d}^* \leftarrow \begin{pmatrix} 1 & \dots & 1 & d_1 \\ 1 & \dots & 1 & d_2 \\ & & \vdots & \\ 1 & \dots & 1 & d_\ell \end{pmatrix} = (d_{i,j}^*)_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq m+1}}$ 
2  $\mathbf{e}^* \leftarrow \begin{pmatrix} 1 & \dots & 1 & e_1 \\ 1 & \dots & 1 & e_2 \\ & & \vdots & \\ 1 & \dots & 1 & e_m \end{pmatrix} = (e_{j,i}^*)_{\substack{1 \leq j \leq m \\ 1 \leq i \leq \ell+1}}$ 
3 for  $i = 1, \dots, \ell$  do
4   for  $j = 1, \dots, m$  do
5      $c \leftarrow \gcd(d_{i,m+1}^*, e_{j,\ell+1}^*)$ 
6      $d_{i,j}^* \leftarrow c$  and  $e_{j,i}^* \leftarrow c$ 
7      $d_{i,m+1}^* \leftarrow d_{i,m+1}^*/c$  and  $e_{j,\ell+1}^* \leftarrow e_{j,\ell+1}^*/c$ 
8   end
9 end
10 remove last column (of all 1's) from  $\mathbf{d}^*$  and  $\mathbf{e}^*$ 
11  $\mathbf{d}^* \leftarrow (d_{i,j}^*)_{\substack{1 \leq k \leq \ell m \\ k=(i-1)m+j \\ 1 \leq i \leq \ell, 1 \leq j \leq m}}$  /* rewrite row-by-row as a sequence */
12  $\mathbf{e}^* \leftarrow (e_{j,i}^*)_{\substack{1 \leq k \leq m \ell \\ k=(j-1)\ell+i \\ 1 \leq j \leq m, 1 \leq i \leq \ell}}$  /* rewrite row-by-row as a sequence */
13 remove all 1's from  $\mathbf{d}^*$  and  $\mathbf{e}^*$ 
14 return  $\mathbf{d}^*, \mathbf{e}^*$ 

```

Conversely, let $\mathbf{d} = (d_1, \dots, d_\ell)$, $\mathbf{e} = (e_1, \dots, e_m)$, and $\ell = \text{len}(\mathbf{d}) \geq \text{len}(\mathbf{e}) = m$. We assume that \mathbf{d} and \mathbf{e} are not associated and define i^* as the minimal index $1 \leq i^* \leq \ell$ such that there is no injective map $\tau: \{1, \dots, i^*\} \rightarrow \{1, \dots, m\}$ with

$$\begin{aligned} d_i &= e_{\tau(i)} \text{ for all } 1 \leq i \leq i^*, \\ \tau(i) < \tau(j) &\text{ for all } 1 \leq i < j \leq i^* \text{ with } \gcd(d_i, d_j) > 1 \end{aligned}$$

in analogy to (3.2) and (3.4), respectively.

We have two possible cases for the execution of the inner loop, steps 4-8, for $i = i^*$.

- If $c = d_{i^*, m+1}^*$ in step 5 for some j , then $e_{j, \ell+1}^* \neq d_{i^*, m+1}^*$ (otherwise, we could extend some injective τ for $i^* - 1$ by $i^* \mapsto j$) and $e_{j, \ell+1}^*$ splits into at least two nontrivial factors in steps 6 and 7, thus $\text{len}(\mathbf{e} \parallel \mathbf{d}) \geq \text{len}(\mathbf{e}) + 1$ and $\mathbf{e} \parallel \mathbf{d} \neq \mathbf{e}$.
- Otherwise $c \neq d_{i^*, m+1}^*$ in step 5 for all j , and $d_{i^*, m+1}^*$ splits into at least two nontrivial factors in steps 6 and 7, thus $\text{len}(\mathbf{d} \parallel \mathbf{e}) \geq \text{len}(\mathbf{d}) + 1$ and $\mathbf{d} \parallel \mathbf{e} \neq \mathbf{d}$.

□

Proposition 3.8. *Let n be a positive integer and \mathbf{d}, \mathbf{e} two ordered factorizations of n with length ℓ and m , respectively. Then the following holds.*

- (i) *Algorithm 3.6 works as specified and requires $O(\ell m)$ gcd-computations and $O(\ell m)$ additional integer divisions.*
- (ii) *We have $\mathcal{D}_{n, \{\mathbf{d}, \mathbf{e}\}} = \mathcal{D}_{n, \{\mathbf{d} \parallel \mathbf{e}, \mathbf{e}\}} = \mathcal{D}_{n, \{\mathbf{d} \parallel \mathbf{e}, \mathbf{e} \parallel \mathbf{d}\}}$.*

Proof. If we ignore the last column of \mathbf{d}^* and \mathbf{e}^* , respectively, we obtain matrices that are each other's transpose before and after every execution of the inner loop in Algorithm 3.6. We use this property to define a sequence of integer matrices $\mathcal{M}^{(k)} \in \mathbb{Z}^{(\ell+1) \times (m+1)}$ for $0 \leq k \leq \ell m$ to simultaneously capture \mathbf{d}^* and \mathbf{e}^* after the inner loop has been executed k times.

For $k = 0$, let

$$\mathcal{M}^{(0)} = \begin{pmatrix} 1 & 1 & \dots & 1 & d_1 \\ 1 & 1 & \dots & 1 & d_2 \\ & & \vdots & & \\ 1 & 1 & \dots & 1 & d_\ell \\ e_1 & e_2 & \dots & e_m & 1 \end{pmatrix} = (m_{i,j}^{(0)})_{\substack{1 \leq i \leq \ell+1 \\ 1 \leq j \leq m+1}}$$

and for $k = (i-1)m + j > 0$, $1 \leq i \leq \ell$, $1 \leq j \leq m$, we define $\mathcal{M}^{(k)}$ as $\mathcal{M}^{(k-1)}$ with $m_{i,j}^{(k-1)}$ replaced by c , $m_{i,m+1}^{(k-1)}$ replaced by $m_{i,m+1}^{(k-1)}/c$, and $m_{\ell+1,j}^{(k-1)}$ replaced by $m_{\ell+1,j}^{(k-1)}/c$, respectively. Thus, we have the following invariants. For every $0 \leq k \leq \ell m$ and every $1 \leq i \leq \ell$, the i th row of $\mathcal{M}^{(k)}$ is a factorization of d_i . Analogously, for every $1 \leq j \leq m$, the j th column of $\mathcal{M}^{(k)}$ is a factorization of e_j .

We have \mathbf{d}^* as $\mathcal{M}^{(k)}$ with the last row removed, and \mathbf{e}^* as $\mathcal{M}^{(k)}$ with the last column removed and then transposed. In particular, the output $\mathbf{d} \parallel \mathbf{e}$ is the first ℓ rows of $\mathcal{M}^{\ell m}$ read as a sequence with 1's ignored. Analogously, the output $\mathbf{e} \parallel \mathbf{d}$ is the first m columns of $\mathcal{M}^{\ell m}$ read as a sequence with 1's ignored.

(i) By the invariants of $\mathcal{M}^{(k)}$ mentioned above, the output $\mathbf{d} \parallel \mathbf{e}$ is a refinement of the input \mathbf{d} . Analogously, the output $\mathbf{e} \parallel \mathbf{d}$ is a refinement of the input \mathbf{e} . The outputs also have the same basis, namely the entries of $\mathcal{M}^{(\ell m)}$ different from 1.

A bijection σ on $\{1, \dots, \ell m\}$ is given by $k = (i-1)m + j \mapsto (j-1)\ell + i$ with $1 \leq i \leq \ell$, $1 \leq j \leq m$. And this satisfies (3.2) since $d_k = c_{i,j} = e_{\sigma(k)}$ for all such i, j . We also show (3.3) for σ . Let $1 \leq k < k' \leq \ell m$ with $k = (i-1)m + j$ and $k' = (i'-1)m + j'$. We have to prove, that if $\sigma(k) > \sigma(k')$, then $\gcd(d_k, d_{k'}) = 1$. The condition is equivalent to $i < i'$ and $j > j'$.

Lemma 3.8a. *Let $1 \leq i \leq m$, $1 \leq j \leq \ell$, $(i-1)m + j \leq k \leq \ell m$ and $c^{(k)}$ the state of Algorithm 3.6 after k executions. Let $R_{i,j} = \prod_{j < j' \leq \ell+1} c_{i,j'}^{(k)}$ and $B_{i,j} = \prod_{i < i' \leq m+1} c_{i',j}^{(k)}$. Then $\gcd(R_{i,j}, B_{i,j}) = 1$. In particular, after the algorithm has terminated, we have $\gcd(c_{i,j'}, c_{i',j}) = 1$ for all $i' > i$, $j' > j$.*

Proof of Lemma 3.8a. Concentrate on the element $c_{i,j'}$. By construction $\prod_{k > j'} c_{i,k}$ and $\prod_{k > i} c_{k,j'}$ are coprime. In particular, their factors $c_{i,j}$ and $c_{i',j'}$. \square

This shows that \mathbf{d}^* and \mathbf{e}^* are associated if we restrict σ to indices k with $d_k > 1$.

Finally, the only arithmetic costs are the gcd-computations in step 5 and the integer divisions in step 7.

(ii) We begin with the first equality. The matrix \mathbf{d}^* corresponds to an ordered factorization, when read row-by-row and 1's ignored. Let $\mathbf{d}^{(k)}$ correspond to the state of the matrix \mathbf{d}^* after the inner loop has been executed exactly k times for $0 \leq k \leq \ell m$. Thus $\mathbf{d}^{(0)} = \mathbf{d}$, $\mathbf{d}^{(\ell m)} = \mathbf{d} \parallel \mathbf{e}$, and we show inductively

$$\mathcal{D}_{n, \{\mathbf{d}^{(k)}, \mathbf{e}\}} = \mathcal{D}_{n, \{\mathbf{d}^{(k+1)}, \mathbf{e}\}} \quad (3.8b)$$

for all $0 \leq k < \ell m$.

Let $k + 1 = (i - 1)m + j$ with $1 \leq i \leq \ell$, $1 \leq j \leq m$. If $c = 1$ in step 5, then $\mathbf{d}^{(k+1)} = \mathbf{d}^{(k)}$ and (3.8b) holds trivially. Otherwise $c > 1$, and $\mathbf{d}^{(k+1)}$ is the proper refinement of $\mathbf{d}^{(k)}$, where the entry $d_{i,m+1}^*$ in $\mathbf{d}^{(k)}$ is replaced by the pair $(c, d_{i,m+1}^*/c)$.

We have to show that if a polynomial has decomposition degree sequences $\mathbf{d}^{(k-1)}$ and \mathbf{e} , then it also has decomposition degree sequence $\mathbf{d}^{(k)}$. This follows from the following generalization of Proposition 2.9.

Lemma 3.8c. *Let $g_1 \circ g_2 \circ \dots \circ g_\ell = h_1 \circ h_2 \circ \dots \circ h_m$ be two decompositions with degree sequence \mathbf{d} and \mathbf{e} , respectively. Let $1 \leq i \leq \ell$, $1 \leq j \leq m$, $c = \gcd(d_i, e_j)$, and*

$$\gcd(d_1 \cdot \dots \cdot d_{i-1} \cdot d_i, e_1 \cdot \dots \cdot e_{j-1}) = \gcd(d_1 \cdot \dots \cdot d_{i-1}, e_1 \cdot \dots \cdot e_{j-1} \cdot e_j). \quad (3.8d)$$

Then there are unique monic original polynomials u and v of degree c and d_i/c , respectively, such that

$$g_i = u \circ v. \quad (3.8e)$$

Therefore, if a monic original polynomial f has decomposition degree sequences \mathbf{d} and \mathbf{e} , then it also has decomposition degree sequence $\mathbf{d}^ = (d_1, \dots, d_{i-1}, c, d_i/c, d_{i+1}, \dots, d_\ell)$.*

Proof of Lemma 3.8c. Let $A = g_1 \circ \dots \circ g_{i-1}$, $B = h_1 \circ \dots \circ h_{j-1}$, and $b = \gcd(\deg(A), \deg(B))$. Then (3.8d) reads $\gcd(\deg(A \circ g_i), \deg(B)) = \gcd(\deg(A), \deg(B \circ h_j))$. This implies $\gcd(\deg(B)/\gcd(\deg(A), \deg(B)), \deg(g_i)) = \gcd(\deg(A)/\gcd(\deg(A), \deg(B)), \deg(h_j))$ and since the first arguments of both outer gcd's are coprime, this quantity is 1. This proves

$$\begin{aligned} \gcd(\deg(A \circ g_i), \deg(B \circ h_j)) &= \gcd(\deg(A), \deg(B)) \cdot \gcd(\deg(g_i), \deg(h_j)) \\ &\quad \cdot \gcd\left(\frac{\deg(A)}{\gcd(\deg(A), \deg(B))}, \frac{\deg(h_j)}{\gcd(\deg(g_i), \deg(h_j))}\right) \\ &\quad \cdot \gcd\left(\frac{\deg(B)}{\gcd(\deg(A), \deg(B))}, \frac{\deg(g_i)}{\gcd(\deg(g_i), \deg(h_j))}\right) \\ &= \gcd(\deg(A), \deg(B)) \cdot \gcd(\deg(g_i), \deg(h_j)) \\ &= bc. \end{aligned} \quad (3.8f)$$

Then Proposition 2.9 applied to left components of the bi-decompositions

$$A \circ (g_i \circ \dots \circ g_\ell) = B \circ (h_j \circ \dots \circ h_m) \quad (3.8g)$$

guarantees the existence of unique, monic original C, A', B' with $\deg(C) = b$ and $\gcd(\deg(A'), \deg(B')) = 1$, such that

$$A = C \circ A' \text{ and } B = C \circ B'. \quad (3.8h)$$

We substitute (3.8h) back into (3.8g), ignore the common left component C due to the absence of equal-degree collisions, and write with the associativity of composition

$$(A' \circ g_i) \circ (g_{i+1} \circ \cdots \circ g_\ell) = (B' \circ h_j) \circ (h_{j+1} \circ \cdots \circ h_m).$$

From (3.8f), we have $\gcd(\deg(A' \circ g_i), \deg(B' \circ h_j)) = \gcd(d_i, e_j) = c$. With Proposition 2.9, we obtain some monic original w and A'' of degree c and $\deg(A' \circ g_i)/c = \deg(A') \cdot d_i/c$, respectively, such that

$$A' \circ g_i = w \circ A''. \quad (3.8i)$$

We have $\gcd(\deg(g_i), \deg(A'')) = d_i/c$ and a final application of Proposition 2.9 to the right components of (3.8i) provides the decomposition for g , claimed in (3.8e). \square

To apply this result with $\mathbf{d} = \mathbf{d}^{(k)}$ and \mathbf{e} , we have to provide (3.8d). For $(k+1) = (i-1)m + j$, we split $D = d_1 \cdot \dots \cdot d_{i-1}$ and $E = e_1 \cdot \dots \cdot e_{j-1}$ into their common (left upper subset) C and the remainders R and B , respectively. By Lemma 3.8a, we have $\gcd(R, B) = 1$ and therefore $\gcd(D, E) = C$. The same lemma shows $\gcd(d_i, B) = 1 = \gcd(R, e_j)$ and we have

$$\gcd(Dd_i, E) = C \gcd(d_i, B) = C \gcd(R, e_j) = \gcd(D, Ee_j),$$

as required for (3.8b).

Finally, interchanging the rôles of \mathbf{d} and \mathbf{e} yields

$$\mathcal{D}_{n, \{\mathbf{d}, \mathbf{e}\}} = \mathcal{D}_{n, \{\mathbf{d} // \mathbf{e}, \mathbf{e}\}} = \mathcal{D}_{n, \{\mathbf{d}, \mathbf{e} // \mathbf{d}\}} = \mathcal{D}_{n, \{\mathbf{d} // \mathbf{e}, \mathbf{e} // \mathbf{d}, \mathbf{d}, \mathbf{e}\}} = \mathcal{D}_{n, \{\mathbf{d} // \mathbf{e}, \mathbf{e} // \mathbf{d}\}},$$

since composition degree sequence $\mathbf{d} // \mathbf{e}$ implies \mathbf{d} and similarly $\mathbf{e} // \mathbf{d}$ implies \mathbf{e} . \square

Example 3.9. Let $n = 7! = 5040$, $\mathbf{d} = (12, 420)$, and $\mathbf{e} = (14, 360)$. We have as refinements

$$\begin{aligned} \mathbf{d} // \mathbf{e} &= (2, 6, 7, 60), \\ \mathbf{e} // \mathbf{d} &= (2, 7, 6, 60), \end{aligned} \quad (3.10)$$

and any $f \in \mathcal{D}_{n, \{\mathbf{d}, \mathbf{e}\}}$ has a unique decomposition $f = a \circ g \circ b$ with $a \in \mathcal{P}_2$, $g \in \mathcal{D}_{42, \{(6,7), (7,6)\}}$, and $b \in \mathcal{P}_{60}$ by Proposition 2.9.

Given a set D with more than two ordered factorizations, we repeatedly replace pairs $d, e \in D$ by $d \parallel e$ and $e \parallel d$, respectively, until we reach a refinement D^* invariant under this operation. This process terminates by Lemma 3.7. The result depends on the order of the applied refinements, but any order ensures the desired properties described by the following proposition.

Proposition 3.11. *Let n be a positive integer and D a set of c ordered factorizations of n . There is a set D^* of at most c ordered factorizations of n with the following properties.*

- (i) *All ordered factorizations of D^* are pairwise associated.*
- (ii) $\mathcal{D}_{n,D^*} = \mathcal{D}_{n,D}$.
- (iii) D^* can be computed from D with at most $O(c^2)$ calls to Algorithm 3.6.

Proof. For $c = 1$, we have $D = \{d\}$ and $D^* = \{d\}$ satisfies all claims.

For $c = 2$, we have $D = \{d, e\}$ for ordered factorizations $d \neq e$, and $D^* = \{d \parallel e, e \parallel d\}$ satisfies all claims by Proposition 3.8.

Let $c > 2$ and $D = \{d^{(1)}, \dots, d^{(c)}\}$. By induction assumption, we can assume all $d^{(i)}$ for $1 \leq i < c - 1$ be pairwise associated. Let $d^{(c)} = f$ and $D^* = \{d^{(1)} \parallel f, d^{(2)} \parallel f, \dots, d^{(c-1)} \parallel f, f \parallel d^{(1)}\}$. Clearly $\mathcal{D}_{n,D} = \mathcal{P}_{n,D^*}$ and it remains to show that all elements of D^* are pairwise associated.

By construction, we have $d^{(1)} \parallel f$ associated with $f \parallel d^{(1)}$ and by transitivity of associatedness the following lemma suffices.

Lemma 3.11a. *If d^* and e^* are associated, then so are $d^* \parallel f$ and $e^* \parallel f$ for any factorization f .*

Proof. Let $\sigma = \sigma(d^*, e^*)$ and compare the matrices

$$\mathcal{M} = \mathcal{M}(d^*, f) \text{ and } \mathcal{N} = \mathcal{M}(e^*, f).$$

The claimed bijection between the indices of \mathcal{M} and \mathcal{N} is given by mapping row i to row $\sigma(i)$ (followed by identity on the columns).

Assume for contradiction that i is the minimal row index such that $\mathcal{M}_{i,*} \neq \mathcal{N}_{\sigma(i),*}$ and j is the minimal column index such that $\mathcal{M}_{i,j} \neq \mathcal{N}_{\sigma(i),j}$.

Let $\mathcal{N}_{\sigma(i),j} = a\mathcal{M}_{i,j}$ with $a > 1$. Then there is a column $j' > j$, such that $a \mid \mathcal{M}_{i,j'}$, since the rows $\mathcal{M}_{i,*}$ and $\mathcal{N}_{\sigma(i),*}$ are both factorizations of $d_i = e_{\sigma(i)}$. Also there is a row $i' > i$, such that $a \mid \mathcal{M}_{i',j}$, since the earlier occurrences of a in that column are pairwise matched.

By Lemma 3.8a, this is a contradiction. And analogously, if $\mathcal{M}_{i,j} = a\mathcal{N}_{\sigma(i),j}$ with $a > 1$. □

□

Any D^* satisfying Proposition 3.11(i)-(ii) is called a *normalization* of D . For a normalized $D = \{d^{(k)} : 1 \leq k \leq c\}$, we have the same basis $\underline{d}^{(k)}$ for all $1 \leq k \leq c$ and call this multiset the *basis* of D , denoted by \underline{D} .

Example 3.12. We add the ordered factorization $f = (20, 252)$ to $D = \{d, e\}$ of Example 3.9 and obtain from (3.10) through refinement with f

$$\begin{aligned} d^* &= (d \parallel e) \parallel f = (2, 2, 3, 7, 5, 12), \\ e^* &= (e \parallel d) \parallel f = (2, 7, 2, 3, 5, 12), \\ f^* &= (f \parallel d) \parallel e = (2, 2, 5, 3, 7, 12). \end{aligned} \tag{3.12b}$$

Any $f \in \mathcal{P}_{n, \{d, e, f\}} = \mathcal{P}_{n, \{d^*, e^*, f^*\}}$ has a unique decomposition $f = a \circ g \circ b$ with $a \in \mathcal{P}_2$, $g \in \mathcal{D}_{210, \{(2,3,7,5), (7,2,3,5), (2,5,3,7)\}}$, and $b \in \mathcal{P}_{12}$. The normalized set $\{d^*, e^*, f^*\}$ has basis $\{2, 2, 3, 5, 7, 12\}$.

3.2 The relation graph of D

An ordered factorization $d = (d_1, d_2, \dots, d_\ell)$ defines a relation \prec_d on its basis $\underline{d} = \{d_1, d_2, \dots, d_\ell\}$ by

$$d_i \prec_d d_j \text{ for } 1 \leq i < j \leq \ell.$$

In other words, $d_i \prec_d d_j$ if d_i appears before d_j in the ordered factorization d , where we distinguish between repeated factors in the multiset \underline{d} . We define the *relation graph* G_d as directed graph with

- vertices $\underline{d} = \{d_1, d_2, \dots, d_\ell\}$ and
- directed edges $(d_j, d_i) = d_i \leftarrow d_j$ for $d_i \prec_d d_j$.

This graph is a *transitive tournament*, that is a complete graph with directed edges, where a path $d \leftarrow e \leftarrow f$ implies an edge $d \leftarrow f$ for any vertices $d, e, f \in \underline{d}$.

Now, let $D = \{d^{(1)}, d^{(2)}, \dots, d^{(c)}\}$ be a normalized set of c ordered factorizations with common basis $\underline{D} = \{d_1, d_2, \dots, d_\ell\}$. The relation \prec_D is the union of the relations $\prec_{d^{(k)}}$ for $1 \leq k \leq c$ and the *relation graph* G_D is the union of the relation graphs $G_{d^{(k)}}$ for $1 \leq k \leq c$. The undirected graph underlying G_D is still complete, but may be intransitive. See Figure 1 for the relation graphs of Example 3.9 and Example 3.12.

We can express the relation \prec_D with the permutations (3.2). Let $\sigma_k = \sigma(d^{(1)}, d^{(k)})$ for $1 \leq k \leq c$. Then σ_1 is the identity on $1, 2, \dots, \ell$ and we have

$$d_i \prec_{d^{(k)}} d_j$$

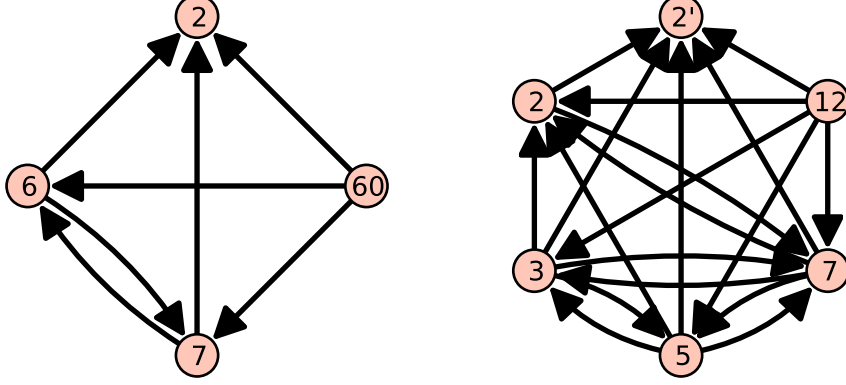


Figure 1: Relation graphs of (3.10) and (3.12b); in the latter, $2'$ denotes the first 2 in each ordered factorization.

if and only if $\sigma_k(i) < \sigma_k(j)$.

A Hamiltonian path $\mathbf{e} = e_1 \leftarrow \cdots \leftarrow e_\ell$ in a graph G visits each vertex exactly once. We call \mathbf{e} *transitive*, if its transitive closure is a subgraph of G . In other words, \mathbf{e} is transitive if $e_i \leftarrow e_j$ is an edge in G for all $1 \leq i < j \leq \ell$. For a relation graph G with vertices d_1, d_2, \dots, d_ℓ and $n = \prod_{1 \leq i \leq \ell} d_i$, we define

$$\mathcal{D}_G = \{f \in \mathcal{P}_n : \text{for every transitive Hamiltonian path } e_1 \leftarrow \cdots \leftarrow e_\ell \text{ in } G, \text{ there is a decomposition } f = g_1 \circ g_2 \circ \cdots \circ g_\ell \text{ with } \deg g_i = e_i \text{ for } 1 \leq i \leq \ell\}.$$

If $G = \{d\}$ is a singleton, we have $\mathcal{D}_G = \mathcal{P}_d$.

Proposition 3.13. *Let n be a positive integer, \mathbf{D} a normalized set of ordered factorizations of n , and G the relation graph of \mathbf{D} . We have*

$$\mathcal{D}_{n, \mathbf{D}} = \mathcal{D}_G.$$

Proof. Every transitive tournament $G_{\mathbf{d}}$ for $\mathbf{d} \in \mathbf{D}$, has \mathbf{d} as its unique transitive Hamiltonian path. Since G is the union of all such $G_{\mathbf{d}}$, we have “ \supseteq ”.

For “ \subseteq ”, we have to show that every polynomial with decomposition degree sequences \mathbf{D} also has decomposition degree sequence \mathbf{d}^* for every transitive Hamiltonian path \mathbf{d}^* in G . We proceed on two levels. First, we derive all transitive Hamiltonian paths in G from “twisting” the paths given by \mathbf{D} . Second, we show that the corresponding “twisted” decomposition degree sequences follow from the given ones.

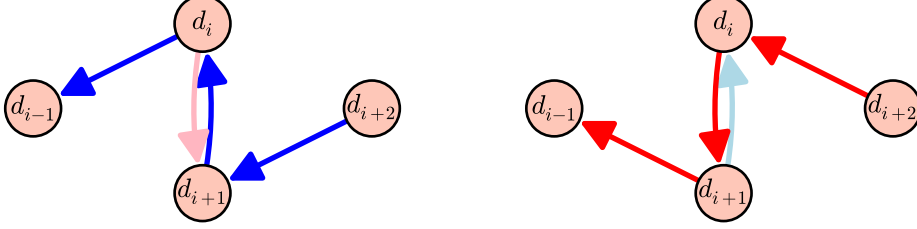


Figure 2: A “swap” between two transitive Hamiltonian paths $d_{i-1} \leftarrow d_i \leftarrow d_{i+1} \leftarrow d_{i+2}$ and $d_{i-1} \leftarrow d_i \leftarrow d_{i+1} \leftarrow d_{i+2}$ along the bidirectional edge between d_i and d_{i+1} .

Let \mathbf{d}^* be a transitive Hamiltonian path in G and $\mathbf{d} \in \mathbf{D}$ arbitrary. We use BUBBLE-SORT to transform \mathbf{d} into \mathbf{d}^* and call the intermediate states after k passes $\mathbf{d}^{(k)}$, $0 \leq k \leq c$, such that $\mathbf{d}^{(0)} = \mathbf{d}$ and $\mathbf{d}^{(c)} = \mathbf{d}^*$.

Algorithm 3.14: BUBBLE-SORT \mathbf{d} according to \mathbf{d}^*

```

1  $\ell \leftarrow \text{len}(\mathbf{d})$ 
2  $k \leftarrow 0, \mathbf{d}^{(0)} \leftarrow \mathbf{d}$ 
3 while  $\mathbf{d}^{(k)} \neq \mathbf{d}^*$  do
4    $k \leftarrow k + 1, \mathbf{d}^{(k)} \leftarrow \mathbf{d}^{(k-1)}$  /* copy previous state */
5   for  $i = 1, \dots, \ell - 1$  do
6      $\sigma = \sigma(\mathbf{d}^{(k)}, \mathbf{d}^*)$ 
7     if  $\sigma(i) > \sigma(i + 1)$  then
8        $(d_i^{(k)}, d_{i+1}^{(k)}) \leftarrow (d_{i+1}^{(k)}, d_i^{(k)})$  /* swap */
9     end
10  end
11 end
12  $c \leftarrow k$ 

```

In other words, $\mathbf{d}^{(k)}$ is obtained from $\mathbf{d}^{(k-1)}$ by at most $\ell - 1$ “swaps” of adjacent vertices. Figure 2 visualizes a swap of $d_i^{(k)}$ and $d_{i+1}^{(k)}$ as in step 8. The fundamental properties of BUBBLE-SORT guarantee correctness and $c \leq \ell(\ell - 1)/2$, see Cormen, Leiserson, Rivest & Stein (2009, Problem 2.2).

Furthermore, the following holds.

- (i) Every pair $(d_i^{(k)}, d_{i+1}^{(k)})$ of swapped vertices in step 8 is connected by a bidirectional edge in G .
- (ii) Every $\mathbf{d}^{(k)}$, $0 \leq k \leq c$, is a transitive Hamiltonian path in G .

For (i), we have the edge $d_i^{(k)} \leftarrow d_{i+1}^{(k)}$ from $\mathbf{d}^{(k-1)}$ and the edge $d_{\sigma(i+1)}^* = d_{i+1}^{(k)} \leftarrow d_i^{(k)} = d_{\sigma(i)}^*$ from \mathbf{d}^* with σ as in step 6.

For $k = 0$, (ii) holds by definition. For $k > 0$ it follows inductively from $k - 1$, since a swap merely replaces the 4-subpath $d_{i-1} \leftarrow d_i \leftarrow d_{i+1} \leftarrow d_{i+2}$ by $d_{i-1} \leftarrow d_{i+1} \leftarrow d_i \leftarrow d_{i+2}$, where the outer edges are guaranteed in G by transitivity of $\mathbf{d}^{(k-1)}$ and the inner edge by (i). Thus, the swapped path is also a transitive Hamiltonian path in G .

Now, we mirror the “swaps” of vertices by “Ritt moves” of components as introduced by Zieve & Müller (2008).

Claim 3.13a (Ritt moves). *Let $g_1 \circ \dots \circ g_\ell = h_1 \circ \dots \circ h_\ell$ be decompositions with degree sequence \mathbf{d} and \mathbf{e} , respectively. Let \mathbf{d} and \mathbf{e} be associated, $\sigma = \sigma(\mathbf{d}, \mathbf{e})$, and $1 \leq i < \ell$ with $\sigma(i) > \sigma(i + 1)$. Then*

$$g_i \circ g_{i+1} = g_i^* \circ g_{i+1}^*$$

with $\deg(g_i) = \deg(g_{i+1}^*)$ and $\deg(g_{i+1}) = \deg(g_i^*)$. Therefore, if some monic original polynomial f has decomposition degree sequences \mathbf{d} and \mathbf{e} , it also has the decomposition degree sequence $\mathbf{d}^* = (d_1, \dots, d_{i-1}, d_{i+1}, d_i, d_{i+2}, \dots, d_\ell)$.

The claim is based on the following lemma.

Lemma 3.13b. *Let \mathbf{d} and \mathbf{e} be associated ordered factorizations, $\sigma = \sigma(\mathbf{d}, \mathbf{e})$, $1 \leq i \leq \text{len}(\mathbf{d})$, and $j = \sigma(i)$. Then*

$$\begin{aligned} \gcd(d_1 \cdot \dots \cdot d_{i-1}, e_1 \cdot \dots \cdot e_{j-1}) &= \gcd(d_1 \cdot \dots \cdot d_{i-1} \cdot d_i, e_1 \cdot \dots \cdot e_{j-1}) \\ &= \gcd(d_1 \cdot \dots \cdot d_{i-1}, e_1 \cdot \dots \cdot e_{j-1} \cdot e_j). \end{aligned}$$

In particular, (3.8d) holds.

Proof of Lemma 3.13b. For any $1 \leq k < j$, with $\gcd(e_k, e_j) = \gcd(e_k, d_i) > 1$, we have $\sigma^{-1}(k) < i$ due to (3.4). In other words, σ^{-1} maps all indices $1 \leq k < j$, where $\gcd(e_k, d_i) > 1$, into the set $\{1, \dots, i - 1\}$. Therefore

$$\begin{aligned} \gcd\left(\frac{e_1 \cdot \dots \cdot e_{j-1}}{\gcd(d_1 \cdot \dots \cdot d_{i-1}, e_1 \cdot \dots \cdot e_{j-1})}, d_i\right) &= 1, \\ \gcd(d_1 \cdot \dots \cdot d_{i-1} \cdot d_i, e_1 \cdot \dots \cdot e_{j-1}) &= \gcd(\gcd(d_1 \cdot \dots \cdot d_{i-1}, e_1 \cdot \dots \cdot e_{j-1}) d_i, e_1 \cdot \dots \cdot e_{j-1}) \\ &= \gcd(d_1 \cdot \dots \cdot d_{i-1}, e_1 \cdot \dots \cdot e_{j-1}). \end{aligned}$$

□

Let $j' = \sigma(i + 1) < \sigma(i) = j$, $A = g_1 \circ \dots \circ g_{i-1}$, $C = g_{i+2} \circ \dots \circ g_\ell$, $A' = h_1 \circ \dots \circ h_{j'-1}$, $B' = h_{j'+1} \circ \dots \circ h_{j-1}$, and $C' = h_{j+1} \circ \dots \circ h_\ell$, such that

$$A \circ g_i \circ g_{i+1} \circ C = A' \circ h_{j'} \circ B' \circ h_j \circ C'.$$

Lemma 3.13b for i and $i + 1$ yields

$$\begin{aligned}\gcd(\deg(A \circ g_i), \deg(A' \circ h_{j'} \circ B')) &= \gcd(\deg(A), \deg(A' \circ h_{j'} \circ B')), \\ \gcd(\deg(A \circ g_i \circ g_{i+1}), \deg(A')) &= \gcd(\deg(A \circ g_i), \deg(A' \circ h_{j'})),\end{aligned}$$

respectively. From the former, we derive

$$\begin{aligned}1 &= \gcd(g_i, \frac{\deg(A' \circ h_{j'} \circ B')}{\gcd(\deg(A), \deg(A' \circ h_{j'} \circ B'))}) \\ &= \gcd(g_i, \frac{\deg(A' \circ h_{j'})}{\gcd(\deg(A), \deg(A' \circ h_{j'}))}).\end{aligned}$$

And then continue the latter as

$$\begin{aligned}&\gcd(\deg(A \circ g_i \circ g_{i+1}), \deg(A')) \\ &= \gcd(\deg(A \circ g_i), \deg(A' \circ h_{j'})) \\ &= \gcd(\deg(A), \deg(A' \circ h_{j'})) \cdot \gcd(g_i, \frac{\deg(A' \circ h_{j'})}{\gcd(\deg(A), \deg(A' \circ h_{j'}))}) \\ &= \gcd(\deg(A), \deg(A' \circ h_{j'})).\end{aligned}\tag{3.13c}$$

Let $G = g_i \circ g_{i+1}$ and $H = h_j$. We have $\gcd(d_i, d_{i+1}) = 1$ due the “twisting condition” $\sigma(i + 1) < \sigma(i)$ and therefore $\gcd(\deg(G), \deg(H)) = d_{i+1}$. We apply Lemma 3.8c with $g_i = G$, $h_j = H$, and $c = d_{i+1}$ in the notation of that claim, and find, since (3.13c) provides condition (3.8d),

$$G = g_i^* \circ g_{i+1}^*$$

with $\deg(g_i^*) = d_{i+1}$ and $\deg(g_{i+1}^*) = d_i$ as required.

Repeated application of Claim 3.13a shows that for every $f \in \mathcal{D}_{n,D}$, $\mathbf{d} \in D$, and every transitive Hamiltonian path \mathbf{d}^* in G , we have $\mathbf{d}^{(k)}$ as in Algorithm 3.14 as decomposition degree sequence. In particular, $\mathbf{d}^{(c)} = \mathbf{d}^*$. \square

3.3 The Decomposition of $\mathcal{D}_{n,D}$

Every directed graph admits a decomposition into strictly connected components, where any two distinct vertices are connected by paths in either direction. Since a relation graph G is the union of directed complete graphs, its strictly connected components G_i , $1 \leq i \leq \ell$, are again relation graphs and form a chain $G_1 \leftarrow G_2 \leftarrow \cdots \leftarrow G_\ell$. Figure 3 shows the connected components of the relation graphs Figure 1

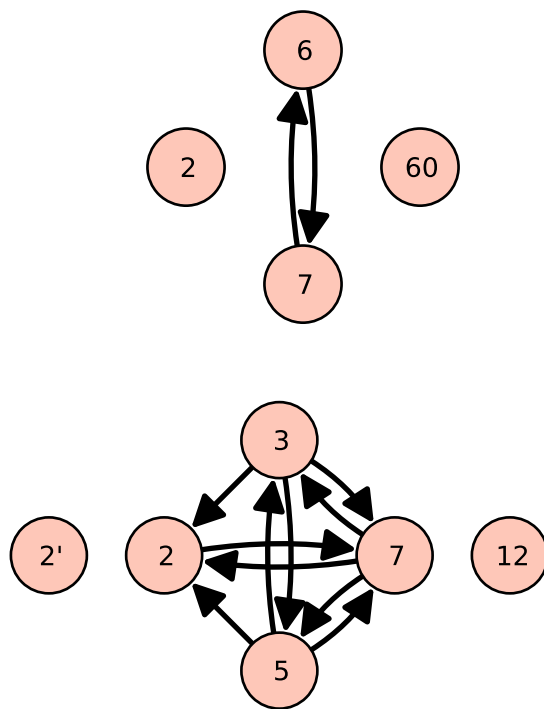


Figure 3: The three strongly connected components of each relation graph in Figure 1, respectively.

Theorem 3.14. *Let G be a relation graph with strongly connected components $G_1 \leftarrow G_2 \leftarrow \cdots \leftarrow G_\ell$. We have*

$$\mathcal{D}_G = \mathcal{D}_{G_1} \circ \mathcal{D}_{G_2} \circ \cdots \circ \mathcal{D}_{G_\ell}$$

and for any $f \in \mathcal{D}_G$, we have uniquely determined $g_i \in \mathcal{D}_{G_i}$ such that $f = g_1 \circ g_2 \circ \cdots \circ g_\ell$. Furthermore, over a finite field $F = \mathbb{F}_q$ with q elements, we have

$$\#\mathcal{D}_G = \prod_{1 \leq i \leq \ell} \#\mathcal{D}_{G_i}.$$

Proof. For $f \in \mathcal{P}_n$, where $n = \prod_{v \in G} v$, we show that the following are equivalent.

- (i) The polynomial f has decomposition degree sequence \mathbf{d} for every transitive Hamiltonian path \mathbf{d} in G .
- (ii) The polynomial f has decomposition degree sequence $\mathbf{d} = \mathbf{d}_1 \leftarrow \mathbf{d}_2 \leftarrow \cdots \leftarrow \mathbf{d}_\ell$ for every concatenation of transitive Hamiltonian paths \mathbf{d}_i in G_i for $1 \leq i \leq \ell$.

Assume (i) and let $\mathbf{d} = \mathbf{d}_1 \leftarrow \mathbf{d}_2 \leftarrow \cdots \leftarrow \mathbf{d}_\ell$ be the concatenation of transitive Hamiltonian paths \mathbf{d}_i in G_i for $1 \leq i \leq \ell$ as in (ii). Then \mathbf{d}_i is a Hamiltonian path in G . Since the underlying undirected graph of G is complete, we have $\mathbf{d}_i \leftarrow \mathbf{d}_j$ in G for any vertices $\mathbf{d}_i \in G_i$ and $\mathbf{d}_j \in G_j$ in distinct strictly connected components with $i < j$. Thus \mathbf{d} is also transitive and f has decomposition degree sequence \mathbf{d} by (i).

Conversely, assume (ii) and observe that the decomposition of G into strictly connected components induces a decomposition of every transitive Hamiltonian path \mathbf{d} in G into Hamiltonian paths \mathbf{d}_i in G_i . These are transitive, since transitivity is a local condition and f has decomposition degree sequence \mathbf{d} by (ii).

Uniqueness and thus the counting formula follow from the absence of equal-degree collisions in the tame case. \square

We split the edge set E of a strictly connected relation graph G with vertices V into its uni-directional edges $\vec{E} = \{(u, v) \in E : (v, u) \notin E\}$ and its bi-directional edges (2-loops) $\overline{E} = \{\{u, v\} \subseteq V : \{(u, v), (v, u)\} \in E\} = E \setminus \vec{E}$. We call the corresponding graphs on V the *directed* and the *undirected* subgraph of G , respectively. The directed subgraph of G is a *directed acyclic graph* since G is the union of transitive tournaments. The undirected subgraph of G is connected. It is also the union of the *permutation graphs* of σ_k , $1 \leq k \leq c$.

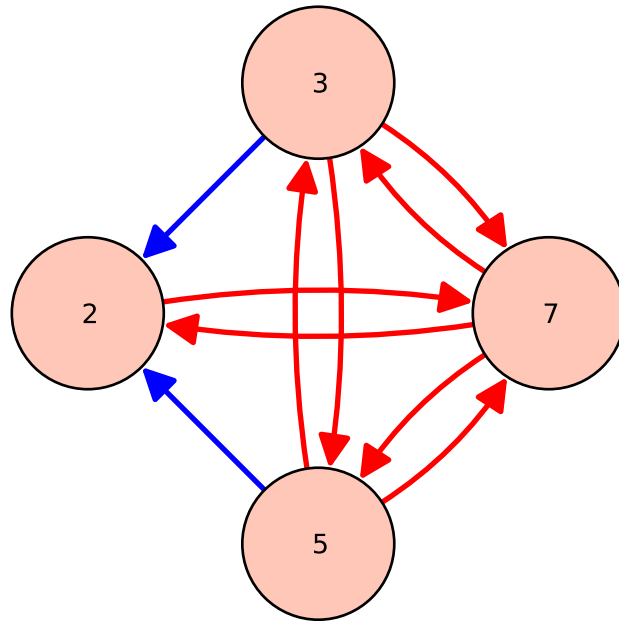


Figure 4: The strongly connected component on 4 vertices of Figure 3 decomposed into its undirected subgraph (red) and its directed subgraph (blue) with MAX-SINK-sorting $7 \prec 2 \prec 5 \prec 3$.

The directed subgraph \vec{G} captures the requirements on the position of the degrees in a decomposition sequence. The undirected subgraph \overline{G} captures the admissible Ritt moves d’après Zieve & Müller (2008) and thus the requirements on the shape of the components.

Every directed acyclic graph admits a *topological sorting* v_1, v_2, \dots, v_ℓ of its vertices, where a directed edge $v_i \leftarrow v_j$ in \vec{G} implies $i < j$, see Cormen *et al.* (2009, Section 22.4). A directed acyclic graph may have several distinct topological sortings. Tarjan (1976) suggested to use DEPTH-FIRST-SEARCH on \vec{G} . The time step, when DEPTH-FIRST-SEARCH visits a vertex for the last time, is called the *finish time* of the vertex and listing the vertices with increasing finish time yields a topological sorting. The result is unique, if the tie-break rule for expanding in DEPTH-FIRST-SEARCH is deterministic. We use the following terminology.

Let $U(v)$ denote the open \overline{G} -neighborhood of a vertex v . It is always nonempty. We call a vertex v *locally maximal*, if its value is greater or equal than the value of every vertex in $U(v)$. Since vertices with equal values are never connected by an edge in \overline{G} , a locally maximal v is always strictly greater than all vertices in $U(v)$. Furthermore, there is at least one locally maximal vertex, namely a “globally” maximal one. There is a unique enumeration of the locally maximal vertices d_1, d_2, \dots, d_m such that

$$d_1 \leftarrow d_2 \leftarrow \dots \leftarrow d_m$$

is a directed path in G . Furthermore, we define for $1 \leq i \leq m$,

$$\begin{aligned} V_i &= U(d_i) \setminus U(d_{i+1}) \text{ and } W_i = V_i \cup \{d_i\}, \\ V_0 &= W_0 = \{v \in G : \text{no edge } d_i \leftarrow v \text{ in } G \text{ for any } 1 \leq i \leq m\}, \\ V_{m+1} &= W_{m+1} = \{v \in G : \text{no edge } v \leftarrow d_i \text{ in } G \text{ for any } 1 \leq i \leq m\}. \end{aligned}$$

The W_i , $0 \leq i \leq m+1$, form a partition of all vertices of \vec{G} and we formulate the tie-break rule for DEPTH-FIRST-SEARCH as follows. Given vertices $u \in W_i$ and $v \in W_j$ with $i < j$, the vertex u is preferred. Given vertices $u, v \in W_i$, the vertex with the larger value is preferred. Since vertices with equal value are always connected by a unidirectional edge in \vec{G} due to (3.4), the search has never to choose between vertices with the same value and DEPTH-FIRST-SEARCH with this tie-break rule yields a unique topological sorting. We call it the MAX-SINK topological sorting of \vec{G} . Figure 4 shows the largest strongly connected component of Figure 3 and its MAX-SINK topological sorting.

Theorem 3.15. *Let G be a strongly connected relation graph with at least two vertices, directed subgraph \vec{G} , and undirected subgraph \overline{G} . Let d_1, d_2, \dots, d_ℓ be the MAX-SINK topological sorting of \vec{G} and let e_i be the product of all vertices in the open \overline{G} -neighborhood of d_i . For every $f \in \mathcal{D}_G$ either (i) or (ii) holds, and (iii) is also valid.*

(i) (Exponential Case) *There are unique $g_i \in \mathcal{E}_{d_i, e_i}$ for $1 \leq i \leq \ell$ and $a \in F$ such that*

$$f = (g_1 \circ g_2 \circ \dots \circ g_\ell)^{[a]}.$$

(ii) (Trigonometric Case) *There are unique $z, a \in F$ with $z \neq 0$ such that*

$$f = T_{d_1 d_2 \dots d_\ell}(x, z)^{[a]}.$$

(iii) *If \overline{G} contains no edge that connects two vertices both larger than 2, then the Trigonometric Case is included in the Exponential Case. Otherwise, they are mutually exclusive.*

Conversely,

$$\mathcal{D}_{n,G} = \mathcal{T}_{d_1 d_2 \dots d_m, 1}^{[F]} \cup (\mathcal{E}_{d_1, e_1} \circ \mathcal{E}_{d_2, e_2} \circ \dots \circ \mathcal{E}_{d_m, e_m})^{[F]}. \quad (3.15a)$$

The e_i are well-defined, since there are no empty neighborhoods in the connected graph \overline{G} with at least two vertices.

Proof. We begin with the proof of existence, then show uniqueness and conclude with the “converse” (3.15a).

The MAX-SINK topological sorting d_1, d_2, \dots, d_ℓ of \vec{G} yields a transitive Hamiltonian path

$$\mathbf{d} = d_1 \prec d_2 \prec \dots \prec d_\ell$$

in G . For the rest of the proof, we identify the MAX-SINK topological sorting with the corresponding transitive Hamiltonian path.

We (re)label the locally maximally vertices d_1, d_2, \dots, d_m and the elements of V_i as $d_i^{(1)}, d_i^{(2)}, \dots, d_i^{(\ell_i)}$ for $0 \leq i \leq m+1$ and $\ell_i = \#V_i$ such that

$$\begin{aligned} \mathbf{d} &= (d_0^{(1)}, \dots, d_0^{(\ell_0)}, d_1, d_1^{(1)}, \dots, d_1^{(\ell_1)}, d_2, d_2^{(1)}, \dots, \\ &\quad d_{m-1}^{(\ell_{m-1})}, d_m, d_m^{(1)}, \dots, d_m^{(\ell_m)}, d_{m+1}^{(1)}, \dots, d_{m+1}^{(\ell_{m+1})}) \\ &= (V_0, d_1, V_1, d_2, \dots, d_m, V_m, V_{m+1}), \end{aligned}$$

where the V_i are read as tuple $(d_i^{(1)}, d_i^{(2)}, \dots, d_i^{(\ell_i)})$. Then f has a decomposition

$$f = G_0^{(1)} \circ \dots \circ G_0^{(\ell_0)} \circ G_1 \circ G_1^{(1)} \circ \dots \circ G_1^{(\ell_1)} \circ G_2 \circ G_2^{(1)} \circ \dots \quad (3.15b) \\ \circ G_{m-1}^{(\ell_{m-1})} \circ G_m \circ G_m^{(1)} \circ \dots \circ G_m^{(\ell_m)} \circ G_{m+1}^{(1)} \circ \dots \circ G_{m+1}^{(\ell_{m+1})}$$

with $G_i^{(j)} \in \mathcal{P}_{d_i^{(j)}}$ for $0 \leq i \leq m+1$, $1 \leq j \leq \ell_i$, and $G_i \in \mathcal{P}_{d_i}$ for $1 \leq i \leq m$.

We assume for the moment that all edges in \overline{G} contain a 2. Then Theorem 2.8 reduces to the exponential case, and we proceed as follows. First, we show that every $G_i^{(j)}$ for $1 \leq i \leq m$, $1 \leq j \leq \ell_i$, is of the form $g_i^{[a_i]}$ for unique $g_i \in \mathcal{E}_{d_i^{(j)}, e_i^{(j)}}$ and unique $a_i \in F$. Then, we extend this to $i = 0$ and $i = m+1$. Finally, we show that the shifting parameters a_i are “compatible” such that a single shifting parameter a suffices.

For every $1 \leq i \leq m$, we use BUBBLE-SORT Algorithm 3.14 with Lemma 3.16 to obtain the decomposition degree sequence

$$(V_0, d_1, V_1, \dots, d_i, V_i, d_i^{(\ell_{i+1})}, \dots, d_i^{(m_i)}, d_{i+1}, \hat{V}_{i+1}, \dots, d_m, \hat{V}_m, V_{m+1}),$$

where $U(d_i) = V_i \cup \{d_i^{(\ell_{i+1})}, \dots, d_i^{(m_i)}\}$ and the latter elements have been omitted from V_{i+1}, \dots, V_m . We have $e_i = \prod_{1 \leq j \leq m_i} d_i^{(j)}$ and this implies the two decomposition degree sequences

$$(V_0, d_1, V_1, \dots, d_i, e_i, d_{i+1}, \hat{V}_{i+1}, \dots, d_m, \hat{V}_m, V_{m+1}), (V_0, d_1, V_1, \dots, e_i, d_i, d_{i+1}, \hat{V}_{i+1}, \dots, d_m, \hat{V}_m, V_{m+1})$$

Thus, there are unique $g_i \in \mathcal{E}_{d_i, e_i}$ and $a_i \in F$ such that in (3.15b), we have

$$G_i \circ G_i^{(1)} \circ \dots \circ G_i^{(\ell_i)} = (g_i \circ x^{d_i^{(1)}} \circ \dots \circ x^{d_i^{(\ell_i)}})^{[a_i]}.$$

The same form applies to $i = 0$, since there is at least one $d_i^{(j)}$ with $1 \leq i \leq m$, $1 \leq j \leq \ell_i$ that is in the \overline{G} -neighborhood of some element of V_0 due to the strong connectedness of G . And since there is no locally maximal element in V_0 all components are of the form $x^{d_0^{(j)}}$ with possible some shift applied. Every connection in G relates the corresponding shifting parameters and since G has a Hamiltonian path, they are all determined by a single choice.

Now, for the general case, where some collisions may be trigonometric, but not exponential. For any two locally maximal vertices d_i and d_j there is some vertex $d \in U(d_i) \cap U(d_j)$. This shows, that either all blocks fall into the exponential case or all blocks fall into the trigonometric case. The two cases are disjoint if and only if there is some edge in \overline{G} that connects two vertices both with value greater than 2.

The stabilizer of original shifting is $\{0\}$ for nonlinear monic original polynomials and there are no equal-degree collisions. Hence the representation is unique.

The converse (3.15a) is a direct computation. \square

Lemma 3.16. *Let $i < j$ and d_j in the open \overline{G} -neighborhood of d_i . Then for every $i < k < j$, we have d_k in the open \overline{G} -neighborhood of d_i or d_j or both.*

Proof. The tournaments underlying G are acyclic. Therefore, if $d_i \prec d_k \prec d_j$ and $d_j \prec d_k$, then at least one other edge is bidirectional, too. \square

4 Exact Counting of Decomposable Polynomials

The classification of Theorem 3.15 yields the exact number of decomposable polynomials at degree n over a finite field \mathbb{F}_q .

Theorem 4.1. *Let G be a strongly connected relation graph with undirected subgraph \overline{G} . Let d_1, d_2, \dots, d_ℓ be the vertices of \overline{G} and e_i be the product of all vertices in the (open) \overline{G} -neighborhood of d_i . Let $\delta_{\overline{G},2}$ be 1 if there is no edge in \overline{G} between two vertices both larger than 2 and let $\delta_{\overline{G},2}$ be 0 otherwise. Then*

$$\#\mathcal{D}_G = \begin{cases} q^{d-1} & \text{if } G = \{d\}, \\ q \cdot (\prod_{d_i \in G} q^{\lfloor d_i/e_i \rfloor} + (1 - \delta_{\overline{G},2}) \cdot (q - 1)) & \text{otherwise.} \end{cases}$$

Proof. For $G = \{d\}$, this follows from (2.1a). Otherwise from the (non)uniqueness of the parameters in Theorem 3.15. \square

We are finally ready to employ the inclusion-exclusion formula (2.4) from the beginning. For a nonempty set D of nontrivial divisors of n , it requires $\#\mathcal{D}_{n,D} = \#\mathcal{D}_{n,\mathbf{D}}$ for $\mathbf{D} = \{(d, n/d) : d \in D\}$. We compute the normalization \mathbf{D}^* by repeated application of Algorithm 3.6 and derive the relation graph of \mathbf{D}^* . Then $\#\mathcal{D}_{n,\mathbf{D}} = \#\mathcal{P}_G$ and the latter follows from Theorem 3.14 and Theorem 4.1.

This is easy to implement, see Algorithm 4.2, and yields the exact expressions for $\#\mathcal{D}_n(\mathbb{F}_q)$ at lightning speed, see Table 1. Where no exact expression was previously known, we compare this to the upper and lower bounds of von zur Gathen (2014a).

Algorithm 4.2: COUNT DECOMPOSABLES

Input: positive integer n
Output: $\#\mathcal{D}_n(\mathbb{F}_q)$ as a polynomial in q for n coprime to q

```

1 if  $n = 1$  or  $n$  is prime then
2   | return 0
3 end
4 total  $\leftarrow 0$ 
5  $N \leftarrow \{1 < d < n : d \mid n\}$ 
6 for  $\emptyset \neq D \subseteq N$  do
7   |  $D \leftarrow \{(d, n/d) : d \in D\}$ 
8   |  $D^* \leftarrow$  normalization of  $D$ 
9   |  $G \leftarrow$  relation graph of  $D^*$ 
10  | collisions  $\leftarrow 1$ 
11  | for strongly connected components  $G_j$  of  $G$  do
12    |  $\overline{G}_j \leftarrow$  undirected subgraph of  $G_j$ 
13    | if  $G_j = \{d\}$  then
14      | connected  $\leftarrow q^d$ 
15    | else
16      |  $\{d_1, d_2, \dots, d_\ell\} \leftarrow G_j$ 
17      | for  $i = 1, \dots, \ell$  do
18        |  $U \leftarrow$  open neighborhood of  $d_i$  in  $\overline{G}_j$ 
19        |  $e_i \leftarrow \prod_{v \in U}$ 
20      | end
21      | connected  $\leftarrow \prod_{d_i \in G_j} q^{\lfloor d_i/e_i \rfloor}$ 
22      | if some edge in  $\overline{G}_j$  connects two vertices both larger than 2 then
23        | connected  $\leftarrow$  connected  $+ q - 1$ 
24      | end
25      | connected  $\leftarrow$  connected  $\cdot q$ 
26    | end
27    | collisions  $\leftarrow$  collisions  $\cdot$  connected
28  | end
29  |  $k \leftarrow \#D$ 
30  | total  $\leftarrow$  total  $+ (-1)^k$  collisions
31 end
32 return total

```

Table 1: Exact values of $\#\mathcal{D}_n(\mathbb{F}_q)$ in the tame case for composite $n \leq 50$, consistent with the upper and lower bounds (in the last column) or exact values (no entry in the last column) of von zur Gathen (2014a, Theorem 5.2).

5 Conclusion

We presented a normal form for multi-collisions of decompositions of arbitrary length with exact description of the (non)uniqueness of the parameters. This lead to an efficiently computable formula for the exact number of such collisions at degree n over a finite field of characteristic coprime to p . We concluded with an algorithm to compute the exact number of decomposable polynomials at degree n over a finite field \mathbb{F}_q in the tame case.

We introduced the relation graph of a set of collisions which may be of independent interest due to its connection to permutation graphs. It would be interesting to characterize sets D of ordered factorizations that lead to identical contributions $\#\mathcal{D}_{n,D}$ and to quickly derive $\#\mathcal{D}_{n,D \cup \{e\}}$ from $\#\mathcal{D}_{n,D}$ or conversely. Finally, this work deals with polynomials only and the study of rational functions with the same methods remains open.

6 Acknowledgements

Many thanks go to Joachim von zur Gathen for useful discussions and pointers to the literature. This work was funded by the B-IT Foundation and the Land Nordrhein- Westfalen.

References

- ROBERTO M. AVANZI & UMBERTO M. ZANNIER (2003). The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$. *Compositio Math.* **139**(3), 263–295. doi:10.1023/B:COMP.0000018136.23898.65.
- ERIC BACH & JEFFREY SHALLIT (1997). *Algorithmic Number Theory, Vol.1: Efficient Algorithms*. MIT Press, Cambridge MA, second printing edition. ISBN 0-262-02405-5.
- DAVID R. BARTON & RICHARD ZIPPEL (1985). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **1**, 159–168.
- RAOUL BLANKERTZ, JOACHIM VON ZUR GATHEN & KONSTANTIN ZIEGLER (2013). Compositions and collisions at degree p^2 . *Journal of Symbolic*

- Computation* **59**, 113–145. ISSN 0747-7171. URL <http://dx.doi.org/10.1016/j.jsc.2013.06.001>. Also available at <http://arxiv.org/abs/1202.5810>. Extended abstract in *Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation ISSAC '12*, Grenoble, France (2012), 91–98.
- ARNAUD BODIN, PIERRE DÈBES & SALAH NAJIB (2009). Indecomposable polynomials and their spectrum. *Acta Arithmetica* **139**(1), 79–100.
- JOHN J. CADE (1985). A New Public-key Cipher Which Allows Signatures. In *Proceedings of the 2nd SIAM Conference on Applied Linear Algebra*. SIAM, Raleigh NC.
- THOMAS H. CORMEN, CHARLES E. LEISERSON, RONALD L. RIVEST & CLIFFORD STEIN (2009). *Introduction to Algorithms*. MIT Press, Cambridge MA, London UK, 3rd edition. ISBN 978-0-262-03384-8 (hardcover), 978-0-262-53305-8 (paperback), 1312 pages .
- F. DOREY & G. WHAPLES (1974). Prime and Composite Polynomials. *Journal of Algebra* **28**, 88–101. URL [http://dx.doi.org/10.1016/0021-8693\(74\)90023-4](http://dx.doi.org/10.1016/0021-8693(74)90023-4).
- H. T. ENGSTROM (1941). Polynomial Substitutions. *American Journal of Mathematics* **63**, 249–255. URL <http://www.jstor.org/stable/pdfplus/2371520.pdf>.
- MICHAEL D. FRIED & R. E. MACRAE (1969). On the invariance of chains of Fields. *Illinois Journal of Mathematics* **13**, 165–171.
- JOACHIM VON ZUR GATHEN (1990a). Functional Decomposition of Polynomials: the Tame Case. *Journal of Symbolic Computation* **9**, 281–299. URL [http://dx.doi.org/10.1016/S0747-7171\(08\)80014-4](http://dx.doi.org/10.1016/S0747-7171(08)80014-4).
- JOACHIM VON ZUR GATHEN (1990b). Functional Decomposition of Polynomials: the Wild Case. *Journal of Symbolic Computation* **10**, 437–452. URL [http://dx.doi.org/10.1016/S0747-7171\(08\)80054-5](http://dx.doi.org/10.1016/S0747-7171(08)80054-5).
- JOACHIM VON ZUR GATHEN (2002). Factorization and Decomposition of Polynomials. In *The Concise Handbook of Algebra*, edited by ALEXANDER V. MIKHALEV & GÜNTER F. PILZ, 159–161. Kluwer Academic Publishers. ISBN 0-7923-7072-4.
- JOACHIM VON ZUR GATHEN (2014a). Counting decomposable univariate polynomials. *To appear in Combinatorics, Probability and Computing*,

- Special Issue*. Extended abstract in *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC '09*, Seoul, Korea (2009). Preprint (2008) available at <http://arxiv.org/abs/0901.0054>.
- JOACHIM VON ZUR GATHEN (2014b). Normal form for Ritt's Second Theorem. *Finite Fields and Their Applications* **27**, 41–71. ISSN 1071-5797. URL <http://dx.doi.org/10.1016/j.ffa.2013.12.004>. Also available at <http://arxiv.org/abs/1308.1135>.
- JOACHIM VON ZUR GATHEN, DEXTER KOZEN & SUSAN LANDAU (1987). Functional Decomposition of Polynomials. In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science*, Los Angeles CA, 127–131. IEEE Computer Society Press, Washington DC. URL <http://dx.doi.org/10.1109/SFCS.1987.29>.
- MARK WILLIAM GIESBRECHT (1988). *Some Results on the Functional Decomposition of Polynomials*. Master's thesis, Department of Computer Science, University of Toronto. Technical Report 209/88. Available as <http://arxiv.org/abs/1004.5433>.
- JOHANNES GRABMEIER, ERICH KALTOFEN & VOLKER WEISPFENNING (editors) (2003). *Computer Algebra Handbook – Foundations, Applications, Systems*. Springer-Verlag, Berlin, Heidelberg, New York. ISBN 3-540-65466-6. URL <http://www.springer.com/978-3-540-65466-7>.
- JAIME GUTIERREZ & DEXTER KOZEN (2003). Polynomial Decomposition. In Grabmeier, Kaltofen & Weispfenning (2003), section 2.2.4 (pages 26–28). URL <http://www.springer.com/978-3-540-65466-7>.
- JAIME GUTIERREZ & DAVID SEVILLA (2006). On Ritt's decomposition theorem in the case of finite fields. *Finite Fields and Their Applications* **12**(3), 403–412. URL <http://dx.doi.org/10.1016/j.ffa.2005.08.004>.
- DEXTER KOZEN & SUSAN LANDAU (1989). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **7**, 445–456. URL [http://dx.doi.org/10.1016/S0747-7171\(89\)80027-6](http://dx.doi.org/10.1016/S0747-7171(89)80027-6). An earlier version was published as Technical Report 86-773, Cornell University, Department of Computer Science, Ithaca, New York, 1986.
- DEXTER KOZEN, SUSAN LANDAU & RICHARD ZIPPEL (1996). Decomposition of Algebraic Functions. *Journal of Symbolic Computation* **22**, 235–246.

- H. LEVI (1942). Composite Polynomials with coefficients in an arbitrary Field of characteristic zero. *American Journal of Mathematics* **64**, 389–400.
- ALICE MEDVEDEV & THOMAS SCANLON (2014). Invariant varieties for polynomial dynamical systems. *Annals of Mathematics* **179**(1), 81–177. URL <http://dx.doi.org/10.4007/annals.2014.179.1.2>. Also available at <http://arxiv.org/abs/0901.2352v3>.
- J. F. RITT (1922). Prime and Composite Polynomials. *Transactions of the American Mathematical Society* **23**, 51–66. URL <http://www.jstor.org/stable/1988911>.
- ANDRZEJ SCHINZEL (1982). *Selected Topics on Polynomials*. Ann Arbor; The University of Michigan Press. ISBN 0-472-08026-1.
- ANDRZEJ SCHINZEL (2000). *Polynomials with special regard to reducibility*. Cambridge University Press, Cambridge, UK. ISBN 0521662257.
- ROBERT ENDRE TARJAN (1976). Edge-Disjoint Spanning Trees and Depth-First Search. *Acta Informatica* **6**, 171–185. URL <http://dx.doi.org/10.1007/BF00268499>.
- PIERRE TORTRAT (1988). Sur la composition des polynômes. *Colloquium Mathematicum* **55**(2), 329–353.
- GERHARD TURNWALD (1995). On Schur’s Conjecture. *Journal of the Australian Mathematical Society, Series A* **58**, 312–357. URL <http://anziamj.austms.org.au/JAMSA/V58/Part3/Turnwald.html>.
- U. ZANNIER (1993). Ritt’s Second Theorem in arbitrary characteristic. *Journal für die reine und angewandte Mathematik* **445**, 175–203.
- UMBERTO ZANNIER (2008). On composite lacunary polynomials and the proof of a conjecture of Schinzel. *Inventiones mathematicae* **174**, 127–138. ISSN 0020-9910 (Print) 1432-1297 (Online). URL <http://dx.doi.org/10.1007/s00222-008-0136-8>.
- MICHAEL E. ZIEVE & PETER MÜLLER (2008). On Ritt’s Polynomial Decomposition Theorems. *Submitted*, URL <http://arxiv.org/abs/0807.3578>.